## CLAIMS

1. A method for data protection, comprising:

accepting data for storage from one or more data sources;

sending the data for storage in a primary storage device and in a secondary storage device;

while awaiting an indication of successful storage of the data in the secondary storage device, temporarily storing a record associated with the data in a disaster-proof storage unit adjacent to the primary storage device; and

when an event damaging at least some of the data in the primary storage device occurs, reconstructing the data using the record stored in the disaster-proof storage unit and at least part of the data stored in the secondary storage device.

2. The method according to claim 1, wherein temporarily storing the record comprises sending an acknowledgement to the one or more data sources responsively to a successful caching of the record in the disaster-proof storage unit, without waiting to receive the indication of the successful storage of the data in the secondary storage device, so as to reduce a transaction latency associated with the storage of the data.

3. The method according to claim 1, wherein temporarily storing the record comprises receiving an acknowledgement from the secondary storage device acknowledging the successful storage of the data in the secondary storage device, and deleting the record from the disaster-proof storage unit responsively to the acknowledgement.

4. The method according to claim 1, wherein reconstructing the data comprises retrieving the disaster-proof storage unit following the event, extracting the record from the disaster-proof storage unit and writing the data associated with the record to the secondary storage device.

5. The method according to claim 4, wherein writing the data comprises remotely connecting the disaster-proof storage unit to the secondary storage device.

6. The method according to claim 1, wherein the disaster-proof storage unit comprises a removable memory device for holding the record, and wherein reconstructing the data comprises, when the disaster-proof storage unit is damaged by the event, removing the memory device from the disaster-proof storage unit and installing the memory device in another unit for readout of the record.

7. The method according to any of claims 1-6, and comprising detecting the event using a detection mechanism in the disaster-proof storage unit, and modifying operation of the disaster-proof storage unit responsively to detecting the event.

8. The method according to claim 7, wherein detecting the event comprises detecting at least one of a loss of external electrical power supply and a communication failure at the disaster-proof storage unit.

9. The method according to claim 7, wherein modifying the operation comprises transmitting the record from the disaster-proof storage unit over a wireless communication link.

10. The method according to claim 7, wherein temporarily storing the record comprises storing the record in two or more disaster-proof storage units, and wherein transmitting the record comprises transmitting two or more different parts of the record respectively from the two or more disaster-proof storage units over respective wireless links so as to shorten a transmission time of the record.

11. The method according to claim 7, wherein modifying the operation comprises transmitting a homing signal from the disaster-proof storage unit, so as to enable location and retrieval of the disaster-proof storage unit.

12. The method according to any of claims 1-6, wherein reconstructing the data comprises:

sensing an environmental condition using an environmental sensor;

predicting the event responsively to the sensed environmental condition; and

after predicting the event, transmitting the record from the disaster-proof storage unit using at least one of a wired connection and a wireless connection.

13. The method according to claim 12, wherein sensing the environmental condition comprises accepting a manual indication from a user that indicates the event.

14. The method according to claim 12, wherein temporarily storing the record comprises sending an acknowledgement message responsively to a successful storage of the record in the disaster-proof storage unit, and comprising, after predicting the event, refraining from sending subsequent acknowledgement messages so as to avoid accepting additional data from the one or more data sources.

15. The method according to claim 12, and comprising, after predicting the event, refraining from sending subsequent data for storage in the primary storage device.

16. The method according to claim 12, and comprising, after predicting the event, temporarily storing in the disaster-proof storage unit only subsequent records associated with data originating from a subset of the one or more data sources.

17. The method according to any of claims 1-6, wherein temporarily storing the record comprises avoiding exceeding a memory capacity in the disaster-proof storage unit by matching the memory capacity with at least one of a maximum allowed size of data pending for acknowledgement by the secondary storage device and a maximum number of write commands pending for storage in the secondary storage device.

18. The method according to any of claims 1-6, wherein temporarily storing the record comprises including in the record additional information related to the data, the additional information comprising at least one of an address of an originating data source, an address of the primary storage device, a time stamp indicating an acceptance time of the data and a storage address intended for the data in the primary storage device.

19. A method for data protection, comprising:

accepting data for storage from one or more data sources;

sending the data for storage in a storage device;

temporarily storing records associated with at least part of the data that is relevant to investigation of disaster events in a disaster-proof storage unit; and

when an event damaging at least some of the data in the storage device occurs, investigating the event using the records stored in the disaster-proof storage unit.

20. The method according to claim 19, wherein the at least part of the data that is relevant to investigation of disaster events comprises at least one of surveillance images, access control information and data originating from a telephony system.

21. The method according to claim 19, wherein the at least part of the data that is relevant to investigation of disaster events comprises data accepted at a time immediately preceding an occurrence of the event.

22. A method for data protection, comprising:

accepting data from a data source for storage in a primary storage device;

periodically sending the data for backup in a backup storage device by means of a sequence of backup operations;

temporarily storing in a disaster-proof storage unit records associated with at least part of the data that is accepted during a time interval between successive backup operations in the sequence; and

when an event damaging at least some of the data in the primary storage device occurs during the time interval, reconstructing the data using the records stored in the disaster-proof storage unit.

23. A method for data protection, comprising:

accepting data for storage from a data source;

sending the data for storage in a primary storage device, while mirroring the data in a secondary storage device;

temporarily storing at least part of the data in a disaster-proof storage unit at a site of the primary storage device; and

when an event damaging at least some of the data in the primary storage device occurs at the site, reconstructing the data using the at least part of the data stored in the disaster-proof storage unit.

24. A system for data protection, comprising:

one or more data sources, which are arranged to send data for storage;

primary and secondary storage devices, which are arranged to hold the data;

a disaster-proof storage unit adjacent to the primary storage device, which is arranged to temporarily store a record associated with the data while awaiting an indication of a successful storage of the data in the secondary storage device, and when an event damaging at least some of the data in the primary storage device occurs, to provide the record so as to enable reconstruction of the data using the record stored in the disaster-proof storage unit and at least part of the data stored in the secondary storage device.

25. The system according to claim 24, and comprising:

an environmental sensor, which is arranged to sense an environmental condition in a vicinity of the primary storage device; and

a processor, which is arranged to predict the event responsively to the sensed environmental condition and, after predicting the event, to instruct the disaster-proof storage unit to transmit the record using at least one of a wired connection and a wireless connection.

26. Apparatus for protecting data sent for storage in primary and secondary storage devices, comprising:

a disaster-proof storage unit, which comprises:

a disaster-proof enclosure, which is arranged to protect components contained therein against disaster events;

a memory device contained in the enclosure, which is arranged to temporarily hold a record associated with the data while awaiting an indication of successful storage of the data in the secondary storage device ; and

a control unit, which is arranged, when an event damaging at least some of the data in the primary storage device occurs, to provide the record so as to enable reconstruction of the data using the record stored in the memory device and at least part of the data stored in the secondary storage device;

a sensor, which is arranged to sense an environmental condition in a vicinity of the primary storage device; and

a protection processor, which is arranged to predict the event responsively to the sensed environmental condition and, responsively to predicting the event, to instruct the disaster-proof storage unit to transmit the record so as to protect the data.

27. The apparatus according to claim 26, wherein the control unit is arranged to delete the record from the memory device responsively to an acknowledgement from the secondary storage device acknowledging the successful storage of the data in the secondary storage device.

28. The apparatus according to claim 26, wherein the control unit is arranged to communicate with the secondary storage device in order to provide the record so as to reconstruct the data.

29. The apparatus according to claim 26, wherein the memory device comprises at least one of a non-volatile memory device and a removable memory device.

30. The apparatus according to any of claims 26-29, wherein the control unit comprises a detection mechanism for detecting the event, and wherein the control unit is arranged to modify operation of the disaster-proof storage unit responsively to detecting the event.

31. The apparatus according to claim 30, wherein the detection mechanism is arranged to detect at least one of a loss of external electrical power supply and a communication failure at the disaster-proof storage unit.

32. The apparatus according to claim 30, wherein the disaster-proof storage unit further comprises a wireless transmitter, which is arranged to transmit the record from the disaster-proof storage unit responsively to detecting the event.

33. The apparatus according to claim 32, wherein the disaster-proof storage unit is one of two or more disaster-proof storage units, which are arranged to transmit respectively two or

more different parts of the record over respective wireless links so as to shorten a transmission time of the record.

34. The apparatus according to claim 30, wherein the disaster-proof storage unit further comprises a homing device, which is arranged to transmit a homing signal from the disaster-proof storage unit responsively to detecting the event, so as to enable location and retrieval of the disaster-proof storage unit.

35. The apparatus according to any of claims 26-29, wherein the record comprises additional information related to the data, the additional information comprising at least one of an address of an originating data source, an address of the primary storage device, a time stamp indicating an acceptance time of the data and a storage address intended for the data in the primary storage device.

36. The apparatus according to any of claims 26-29, wherein the sensor is arranged to accept a manual indication from a user so as to predict the event.

37. The apparatus according to any of claims 26-29, wherein the data is accepted from one or more data sources, and wherein the protection processor is arranged to send an acknowledgement message responsively to a successful storage of the record in the disaster-proof storage unit and to refrain from sending subsequent acknowledgement messages after predicting the event so at to avoid accepting additional data from the one or more data sources.

38. The apparatus according to any of claims 26-29, wherein the data is accepted from one or more data sources, and wherein the protection processor is arranged to control a rate of the data accepted from the one or more data sources after predicting the event.

39. The apparatus according to any of claims 26-29, wherein the data is accepted from one or more data sources, and wherein the protection processor is arranged to send for temporary storage in the disaster-proof storage unit only subsequent records associated with data originating from a subset of the one or more data sources after predicting the event.

40. The apparatus according to any of claims 26-29, wherein a capacity of the memory device is matched to a maximum allowed size of data pending for acknowledgement by the secondary storage device so as to avoid exceeding the memory capacity.

41. A computer software product for data protection, the product comprising a computer-readable medium, in which program instructions are stored, which instructions, when read by a computer, cause the computer to accept data from one or more data sources sent for storage

in primary and secondary storage devices, and to temporarily store a record associated with the data in a disaster-proof storage unit adjacent to the primary storage device, while awaiting an indication of successful storage of the data in the secondary storage device.